

FICHIER DE RENSEIGNEMENTS PERSONNELS

Tel que le prescrit l'article 76 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1), le Musée de la civilisation (MCQ) rend publiques certaines informations concernant ce fichier contenant des informations personnelles telles que définies par l'article 54 de la même loi.

Date de l'analyse	2024-09-09	☐ Première déclaration ☒ Modification ☐ Destruction
--------------------------	------------	---

1. IDENTIFICATION DU FICHIER

Désignation : Accès à l'information et protection des renseignements personnels

Description : Documents relatifs à la gestion des demandes d'accès aux documents et aux informations institutionnels du Musée, en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

2. CATÉGORIES DE RENSEIGNEMENTS CONTENUS DANS LE FICHIERⁱ

☒ Identification	☐ Situation sociale/Familiale
☐ Santé	☐ Génétique/Biométrie
☐ Financier	☐ Vie ou orientation sexuelle
☒ Relatif au travail	☐ Convictions religieuses
☒ Scolaire	☐ Opinions politiques
☐ Démographique	☐ Origine ethnique ou raciale
☐ Autre(s) (spécifier) : Cliquez ou appuyez ici pour entrer du texte.	

Remarques : Cliquez ou appuyez ici pour entrer du texte.

3. FINS POUR LESQUELLES LES RENSEIGNEMENTS SONT CONSERVÉS

☒	Application d'une loi	Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1.
☐	Application d'un règlement	Spécifier.
☐	Application d'un programme	Spécifier.
☐	Gestion interne du MCQ	
☐	Statistiques	
☐	Autre(s) fin(s)	Spécifier.

4. MODE DE GESTION DU FICHIER

4.1 Supports physiques locaux : ☐ a. Manuel (papier, carton, etc.) ☐ b. Mécanique (microfiche, microfilm, etc.) ☒ c. Informatique (disque, bande, etc.)		4.2 Supports délocalisés : ☐ d. Infonuagique	
Localisation dans un endroit unique :	☐ Oui	☒ Non	
Applications et logiciels (informatique, infonuagique)	Serveurs du Musée et logiciel de traitement des courriels		
Durée générale de conservation des renseignements :	Jusqu'à l'épuisement des recours légaux et par la suite, 5 ans en statut semi actif.		
Remarques : Cliquez ou appuyez ici pour entrer du texte.			

5. PROVENANCE DE L'INFORMATION VERSÉE AU FICHIER

☒	La personne concernée	☐	Une autre personne physique	☐	Un membre du personnel du MCQ
-------------------------------------	-----------------------	--------------------------	-----------------------------	--------------------------	-------------------------------

☐	Un autre organisme public que le MCQ	☒	Un organisme privé	
☐	Autre(s) (spécifier) :			

6. CATÉGORIES DE PERSONNES CONCERNÉES PAR LES RENSEIGNEMENTS VERSÉS AU FICHIER

☒ a. Les clientèles du MCQ	☐ b. Le personnel du MCQ
☐ Autre(s) :	Spécifier.

7. CATÉGORIES DE PERSONNES AYANT ACCÈS AU FICHIER DANS L'EXERCICE DE LEURS FONCTIONS

☒ Présidence-direction générale ☐ Gestionnaires ☒ Membres du personnel de la direction de l'administration et du secrétariat général ☐ Membres du personnel du service des finances ☐ Membres du personnel de la direction des ressources humaines ☐ Membres du personnel de la direction des collections ☐ Membres du personnel de la direction de l'accueil et de l'expérience du visiteur ☐ Membres du personnel de la direction de la programmation ☐ Membres du personnel de la direction de la mise en marché et du mécénat ☐ Membres du personnel de la direction des immobilisations, du numériques et des technologies ☐ Membres du personnel de la direction du développement et de l'innovation ☐ Autres : Spécifier.

8. MESURES DE SÉCURITÉ PRISES POUR ASSURER LA PROTECTION DES RENSEIGNEMENTS PERSONNELSⁱⁱ

8.1 Pour un fichier manuel ou mécanique

- ☐ a. Contrôle des entrées / sorties de personnes
- ☐ b. Contrôle physique des locaux / installations
- ☐ c. Contrôle à l'utilisation du document
- ☐ d. Contrôle des procédures
- ☐ e. Destruction confidentielle
- ☐ f. Signature d'une entente de confidentialité
- ☐ g. Vérification de l'intégrité du personnel
- ☐ h. Autre(s) (spécifier) : n/a

8.2. Pour un fichier informatique ou hébergé en infonuagique

- ☒ a. Contrôle préventif de l'accès au fichier
- ☐ b. Journaux de vérification des données
- ☐ c. Règles et pratiques de vérification des logiciels
- ☒ d. Mesures liées aux outils informatiques
- ☐ e. Règles et pratiques de vérification du fichier
- ☐ f. Destruction confidentielle
- ☐ g. Signature d'une entente de confidentialité
- ☐ h. Vérification de l'intégrité du personnel
- ☐ i. Autre(s) (spécifier) :

ⁱ Les définitions se retrouvent sur le site du Gouvernement du Québec : [Présentation des concepts-clés liés aux renseignements personnels](#)

ii Précisions :

- 8.1 a. Contrôle des entrées / sorties de personnes : Mécanisme de contrôle de l'accès aux installations (ex. : carte magnétique).
- 8.1 b. Contrôle physique des locaux / installations : Verrouillage des espaces et/ou équipements de rangement.
- 8.1 c. Contrôle à l'utilisation du document : Mécanisme permettant de contrôler qui consulte un document.
- 8.1 d. Contrôle des procédures : Mise en place de procédures d'accès aux documents.
- 8.1 e. Destruction confidentielle : Élimination sécurisée des documents.
- 8.1 f. Signature d'une entente de confidentialité : Signature par l'utilisateur d'un engagement à garder strictement confidentiels les renseignements consultés.
- 8.1 g. Vérification de l'intégrité du personnel : Approbation lors de l'embauche ou de l'entrée en fonction dans des affectations associées à la manipulation ou à la consultation des documents.
- 8.2 a. Contrôle préventif de l'accès au fichier : Attribution d'un identifiant et d'un mot de passe, environnement réseau sécurisé.
- 8.2 b. Journaux de vérification des données : Vérification des accès aux fichiers.
- 8.2 c. Règles et pratiques de vérification des logiciels : Processus permettant de vérifier et de maintenir la pérennité, l'efficacité et la sécurité des logiciels utilisés.
- 8.2 d. Mesures liées aux outils informatiques : Mesures assurant le maintien et l'entretien de l'équipement informatique, y compris l'emplacement sécurisé de ce dernier.
- 8.2 e. Règles et pratiques de vérification du fichier : Processus permettant de s'assurer que la signature électronique du fichier demeure la même (veille des modifications ou suppressions).
- 8.2 f. Destruction confidentielle : Élimination sécurisée des fichiers ou des données.
- 8.2 g. Signature d'une entente de confidentialité : Signature par l'utilisateur d'un engagement à garder strictement confidentiels les fichiers ou les données consultés.
- 8.2 h. Vérification de l'intégrité du personnel : Approbation lors de l'embauche ou de l'entrée en fonction dans des affectations associées à la manipulation ou à la consultation des fichiers ou données.